ARITHMETIC DIFFERENTIAL OPERATORS ON $\mathbb{Z}_p$

ALEXANDRU BUIUM, CLAIRE C. RALPH, AND SANTIAGO R. SIMANCA

Abstract. Given a prime p, we let $\delta x = (x - x^p)/p$ be the the Fermat quotient operator over $\mathbb{Z}_p$. We prove that a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is analytic if, and only if, there exists m such that f can be represented as $f(x) = F(x, \delta x, \ldots, \delta^m x)$, where F is a restricted power series with $\mathbb{Z}_p$-coefficients in $m + 1$ variables.

1. Introduction

1.1. **Main results.** An arithmetic analogue of the theory of ordinary differential equations was initiated in [3], and further developed in a series of subsequent publications; see [1], and the bibliography therein. In this theory, the role of the differentiation operator is played by a Fermat quotient operator acting on numbers. Later on, the theory was extended to one of arithmetic partial differential equations [6, 7, 5]. Our work here derives its motivation from certain examples encountered in the original development of the theory, but is independent of them.

Let p be a prime integer that we fix hereafter. We denote by $\mathbb{Q}_p$ the field of p-adic numbers, with p-adic norm $\|\cdot\|_p$ normalized by $\|p\|_p = p^{-1}$. On the ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$ of p-adic integers, we consider the *Fermat quotient operator*

$$\delta a = \frac{a - a^p}{p}\,, \tag{1}$$

which by analogy we view as the "derivative of a with respect to p." We denote by δ^i the i-th iterate of δ.

Given a multi-index $\alpha = (\alpha_0, \ldots, \alpha_k)$ of non-negative integers, we shall say that $\alpha \geq 0$, and use the expression x^α to denote the monomial $x_0^{\alpha_0} \cdots x_k^{\alpha_k}$. By $|\alpha|$ we mean $|\alpha| = \alpha_0 + \cdots + \alpha_k$. We recall that $F(x) = \sum_{\alpha \geq 0} a_\alpha x^\alpha \in \mathbb{Z}_p[[x_0, \ldots, x_k]]$ is said to be a *restricted* power series if $\lim_{|\alpha| \to \infty} a_\alpha = 0$.

Definition 1. A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is called an *arithmetic differential operator of order m* if there exists a restricted power series $F \in \mathbb{Z}_p[[x_0, x_1, \ldots, x_m]]$ such that

$$f(a) = F(a, \delta a, \ldots, \delta^m a) \tag{2}$$

for all $a \in \mathbb{Z}_p$. We say that the series F *δ-represents* f. □

Definition 2. A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be *analytic of level m*, if for any $a \in \mathbb{Z}_p$ there exists a restricted power series $F_a \in \mathbb{Z}_p[[x]]$ such that

$$f(a + p^m u) = F_a(u)$$

for all $u \in \mathbb{Z}_p$. We say that the collection of series F_a *represents* f. □

During the preparation of this work, the first author was partially supported by NSF grant DMS 0552314.

Remark 3. We have the following simple observations:

(1) In Definition 2, it is enough to take the as in a complete residue system mod p^m in $\mathbb{Z}_p$.
(2) A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is analytic in the sense of [10] (cf. with [11], p. LG 2.4) if, and only if, it is analytic of level m for some m.
(3) If $f, g : \mathbb{Z}_p \to \mathbb{Z}_p$ are arithmetic differential operators of orders m and n, respectively, then $f \circ g$ is an arithmetic differential operator of order $m+n$.
(4) Any arithmetic differential operator $\mathbb{Z}_p \to \mathbb{Z}_p$ is an analytic function in the sense of [10, 11]. □

It will be relatively easy to sharpen the last part of this remark to the following:

Theorem 4. *Any arithmetic differential operator $f : \mathbb{Z}_p \to \mathbb{Z}_p$ of order m is an analytic function of level m.*

Our main result says that the converse of this statement is true:

Theorem 5. *Any analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ of level m is an arithmetic differential operator of order m.*

Remark 6. Actually, we will also prove that among the restricted power series that δ-represent f, there is a unique one $F = F(x_0, \ldots, x_m)$ satisfying the condition that all of its monomials are of degree less or equal that $p-1$ in each of the variables $x_0, \ldots, x_{m-1}$; cf. Theorem 13. We call this F the *canonical* series δ-representing f. As the proof of Theorem 13 will show, the computation of the canonical series F δ-representing f in terms of the collection of series F_a representing f is a rather non-trivial task.

Remark 7. The context of our work here and that of the theory in [1, 3] differ from each other. Indeed, in [1, 3] the ring $\mathbb{Z}_p$ is replaced by the completion R of the maximum unramified extension of $\mathbb{Z}_p$, and our δ here is replaced by

$$\begin{array}{ccc} R & \stackrel{\delta}{\to} & R \\ a & \mapsto & \dfrac{\phi(a) - a^p}{p}, \end{array}$$

where ϕ is the unique lift of Frobenius on R. In this other setting, an arithmetic differential operator that is not of order 0 is never analytic, and an analytic function that is not of level 0 is never an arithmetic differential operator. The difference between the theories over these two rings is, in some sense, analogous to the difference between number theoretic statements about finite fields and algebraic geometric statements over their algebraic closures. □

Remark 8. If we use a slightly more general context, the theory in [1, 3] gives rise to several interesting number theoretic locally constant functions that have nice representations as arithmetic differential operators of low order. As these have been the main source of motivation for our work, we describe briefly two of them here.

Definition 1 can be extended by considering functions $f : \mathbb{Z}_p^N \to \mathbb{Z}_p$ that can be represented as in (2) with an $F \in \mathbb{Z}_p[[x_0, \ldots, x_m]]$ but where now each x_j is an N-tuple of variables. We call these *arithmetic differential operators of order m* also. If X is an affine scheme embedded into the affine N-space over $\mathbb{Z}_p$, we let $X(\mathbb{Z}_p) \subset \mathbb{Z}_p^N$ be the natural inclusion at the level of $\mathbb{Z}_p$-points. Then a function

$X(\mathbb{Z}_p) \to \mathbb{Z}_p$ is called an *arithmetic differential of order* m if it can be extended to an arithmetic differential operator $\mathbb{Z}_p^N \to \mathbb{Z}_p$ of order m.

For instance, let X be the multiplicative group scheme over $\mathbb{Z}_p$ embedded into the affine plane $\operatorname{Spec} \mathbb{Z}_p[v, w]$ via the map $u \mapsto (u, u^{-1})$. The we have that $X(\mathbb{Z}_p) = \mathbb{Z}_p^\times$, and we can talk about arithmetic differential operators $\mathbb{Z}_p^\times \to \mathbb{Z}_p$ of order m. As noted in [4], for odd primes p, the *Legendre symbol* $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p$, defined by

$$f(a) := \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \pmod p \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \pmod p \text{ is a quadratic nonresidue mod } p, \end{cases}$$

is the arithmetic differential operator of order one given by

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \left(1 + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(2n-2)! p^n}{2^{2n-1}(n-1)! n!} (\delta a)^n (a^{-1})^{-pn}\right).$$

This function is locally constant of level 1, that is to say, constant on discs of radius $1/p$.

Similarly, let X be the locus in the plane $\operatorname{Spec} \mathbb{Z}_p[u, v]$ over $\mathbb{Z}_p$, where $4v^3 + 27w^2$ is invertible, and view X as embedded in 3-space via the map $(v, w) \mapsto (v, w, (4v^3 + 27w^2)^{-1})$. Consider the traces of Frobenii of the reductions mod p of elliptic curves $y^2 = x^3 + Ax + B$ over $\mathbb{Z}_p$. These functions can be represented as quotients of some remarkable arithmetic differential operators of order 2 defined on

$$X(\mathbb{Z}_p) = \{(A, B) \in \mathbb{Z}_p \times \mathbb{Z}_p : \, 4A^3 + 27B^2 \in \mathbb{Z}_p^\times\}.$$

Cf. [4] for details. □

1.2. **Continuous functions on $\mathbb{Z}_p$.** It is of interest to compare our results with a known Mahler-type theorem about the structure of continuous $\mathbb{Z}_p$-valued functions on $\mathbb{Z}_p$.

Let A be the set of all non-negative integral vectors $\alpha = (\alpha_0, \alpha_1, \alpha_2, \ldots)$ with finite support. Thus, $\alpha_j \geq 0$ for all j, and $\alpha_j = 0$ for j sufficiently large. If $\alpha \in A$, it makes sense to compute $|\alpha|$. Given a sequence of variables $x_0, x_1, x_2, \ldots$, we set x^α for $x_0^{\alpha_0} x_1^{\alpha_1} x_2^{\alpha_2} \ldots$. Then we say that a power series

$$F(x_0, x_1, x_2, \ldots) = \sum_{\alpha \in A} a_\alpha x^\alpha \,, \; a_\alpha \in \mathbb{Z}_p \,,$$

is *restricted* if $\lim_{|\alpha| \to \infty} a_\alpha = 0$.

Let us now recall the following Mahler-type theorem, a special case of results in [8, 2, 9]:

Theorem 9. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a continuous function. Then there exists a restricted power series $F(x_0, x_1, x_2, \ldots)$ in the variables $x_0, x_1, x_2, \ldots$, with $\mathbb{Z}_p$-coefficients, such that*

$$f(a) = F(a, \delta a, \delta^2 a, \ldots)$$

for all a in $\mathbb{Z}_p$. □

Our Theorems 4 and 5 imply that the series F in Theorem 9 can be chosen to depend on finitely many variables if, and only if, f is analytic.

1.3. **Structure of the paper.** In §2 we prove the basic p-adic estimates we shall need in our work, and follow that by proving Theorem 4 in §3. In §4 we introduce a matrix intrinsically associated to the number p^m, and analyze its determinant. They play an important rôle in the proof of Theorem 5, which we do in §5.

2. p-ADIC ESTIMATES

Lemma 10. *If $a \in \mathbb{Z}_p$ and $x = a + p^n u$ in the disc $a + p^n\mathbb{Z}_p$, write $\delta^k x$ as a polynomial function of u of degree p^k,*

$$\delta^k x = \sum_{j=0}^{p^k} c_{a,j}^k u^j \,,$$

with $c_{a,j} \in \mathbb{Q}_p$. Then we have the following p-adic estimates:

(1) $\left\| c_{a,0}^k \right\|_p \leq 1$.
(2) $\left\| c_{a,1}^k \right\|_p = \frac{1}{p^{n-k}}$.
(3) $\left\| c_{a,j}^k \right\|_p \leq \frac{1}{p^{(n-k+1)j-1}}\,, \quad 2 \leq j \leq p^k\,.$

Proof. Assertion (1) follows from the equality $c_{a,0}^k = \delta^k a$. We prove assertions (2) and (3) by induction on k. The result is clear for $k = 0$. Assuming that it holds for $k-1$, we prove it for k.

By hypothesis we have that

$$\delta^{k-1} x = \sum_{j=0}^{p^{k-1}} c_{a,j}^{k-1} u^j \,,$$

where for $j \geq 1$ the coefficients $c_{a,j}^{k-1}$ satisfy the estimates

$$\left\| c_{a,j}^{k-1} \right\|_p \leq \frac{1}{p^{(n-k+2)j-1}}\,,$$

with equality for $j = 1$. We use (1) to write the k-th iterate as

$$\delta^k x = \sum_{j=0}^{p^k} c_{a,j}^k u^j = \frac{\sum_{j=0}^{p^{k-1}} c_{a,j}^{k-1} u^j - (\sum_{j=0}^{p^{k-1}} c_{a,j}^{k-1} u^j)^p}{p}\,.$$

Consider a fixed index $j \geq 1$. It follows that $c_{a,j}^k$ is equal to $c_{a,j}^{k-1}/p$ minus a sum of elements of the form a rational integer times

$$\frac{c_{a,j_1}^{k-1} \cdots c_{a,j_p}^{k-1}}{p}\,,$$

where $j_1 + \cdots + j_p = j$. By a commutation, we may assume that there is an s such that $j_1, \ldots, j_s \geq 1$ and $j_t = 0$ for $t > s$. Then $s \leq j_1 + \cdots + j_s = j$, and by assertion (1) of the Lemma and the induction hypothesis applied to each of the factors, we conclude that

$$\left\| \frac{c_{a,j_1}^{k-1} \cdots c_{a,j_p}^{k-1}}{p} \right\|_p \leq \left\| \frac{c_{a,j_1}^{k-1} \cdots c_{a,j_s}^{k-1}}{p} \right\|_p \leq \frac{1}{p^{(n-k+2)(j_1+\cdots+j_s)-s-1}} \leq \frac{1}{p^{(n-k+1)j-1}}\,,$$

and the estimate in (3) follows. The equality in Assertion (2) follows from the induction hypothesis and the identity

$$c_{a,1}^k = c_{a,1}^{k-1} \left(\frac{1}{p} - (c_{a,0}^{k-1})^{p-1} \right)\,.$$

This completes the proof. □

3. Proof of Theorem 4

Let $f(x) = F(x, \delta x, \dots, \delta^m x)$ by an operator of order m given by the restricted power series $F \in \mathbb{Z}_p[[t_0, \dots, t_m]]$. Thus,

$$f(x) = \sum_{\alpha=(\alpha_0,\dots,\alpha_m)} a_\alpha x^{\alpha_0} (\delta x)^{\alpha_1} \cdots (\delta^m x)^{\alpha_m} ,$$

where $a_\alpha \to 0$ p-adically as $|\alpha| \to \infty$.

Let $I = \{0, 1, \dots, p^m - 1\}$. The family of discs $\{a + p^n \mathbb{Z}_p\}_{a \in I}$ forms a covering of $\mathbb{Z}_p$. By Lemma 10, if $a \in I$ we have that $f(a + p^m u) = F_a(u)$, where

$$F_a(u) = \sum_{\alpha=(\alpha_0,\dots,\alpha_r)} a_\alpha \Big(\sum_{j_0=0}^{p^0} c^0_{a,j_0} u^{j_0}\Big)^{\alpha_0} \Big(\sum_{j_1=0}^{p^1} c^1_{a,j_1} u^{j_1}\Big)^{\alpha_1} \cdots \Big(\sum_{j_r=0}^{p^m} c^m_{a,j_m} u^{j_m}\Big)^{\alpha_m} ,$$

with all the c^k_{a,j_l}s in $\mathbb{Z}_p$. Notice that $F_a(u)$ is a power series in u with $\mathbb{Z}_p$-coefficients that go to zero p-adically as $|\alpha| \to \infty$. □

4. A matrix associated to p^m

Let us consider the set of all p-adic integer roots of the function $x \mapsto \delta^m x$:

$$C_m := \{a \in \mathbb{Z}_p : \delta^m a = 0\} .$$

Since the m-th iterate of δ is given by a polynomial of degree p^m with $\mathbb{Q}_p$-coefficients, C_m has at most p^m elements. In fact, it has exactly p^m elements. We have:

Lemma 11. *The composition*

$$C_m \subset \mathbb{Z}_p \to \mathbb{Z}_p / p^m \mathbb{Z}_p$$

is bijective.

Proof. We proceed by induction on m. For $m = 0$ we have that $C_0 = \{0\}$. We assume now that the statement is true for $m - 1$, and prove it for m.

Given $a \in C_{m-1}$, we consider the polynomial $t^p - t + pa \in \mathbb{Z}_p[t]$. By Hensel's lemma, it has p distinct roots that we denote by $a_1, \dots, a_p \in \mathbb{Z}_p$. Notice that we have $\delta a_j = a$ for all js, and since $\delta^{m-1} a = 0$, it follows that $\delta^m a_j = 0$. We claim that if $a, a' \in C_{m-1}$ and we have that

$$a_j \equiv a'_{j'} \mod p^m , \tag{3}$$

for some j, j', then $a = a'$ and $j = j'$. Indeed, if (3) holds then $a \equiv a' \bmod p^{m-1}$, and by the induction hypothesis, $a = a'$ and hence $j = j'$ as well. By this claim and the induction hypothesis, C_m contains a set of p^m elements that injects into $\mathbb{Z}_p / p^m \mathbb{Z}_p$. As C_m has at most p^m elements, this forces the map $C_m \to \mathbb{Z}_p / p^m \mathbb{Z}_p$ to be bijective. □

By Lemma 11, we can write

$$C_m = \{a_0, a_1, \dots, a_{p^m - 1}\} , \tag{4}$$

where $a_\alpha \equiv \alpha \bmod p^m$ for all αs in the set

$$I = \{0, \dots, p^m - 1\} . \tag{5}$$

On the other hand, let us fix an ordering in the set

$$I' = \{\beta = (\beta_0, \dots, \beta_{m-1}) \in \mathbb{Z}^m : 0 \le \beta_0, \dots, \beta_{m-1} \le p - 1\} , \tag{6}$$

and consider the $(p^m-1)\times(p^m-1)$-matrix

$$W=(w_{\alpha\beta})_{\alpha\in I,\beta\in I'}\,, \tag{7}$$

whose entries are given by

$$w_{\alpha\beta}:=(a_\alpha)^{\beta_0}(\delta a_\alpha)^{\beta_1}\dots(\delta^{m-1}a_\alpha)^{\beta_{m-1}}\in\mathbb{Z}_p\,,$$

where we have used the convention that $a^0=1$ for all $a\in\mathbb{Z}_p$. Up to a permutation of its columns, the matrix W is intrinsically associated to the number p^m.

Lemma 12. *The determinant of the matrix W is invertible in $\mathbb{Z}_p$.*

Proof. We use the reduction mod p mapping

$$\begin{array}{ccc}\mathbb{Z}_p & \to & \mathbb{F}_p:=\mathbb{Z}_p/p\mathbb{Z}_p\\ a & \mapsto & \overline{a}\end{array}\,.$$

By Lemma 3.20 in [1], the function

$$\begin{array}{ccc}\mathbb{Z}_p & \to & \mathbb{F}_p^m\\ a & \mapsto & (\overline{a},\overline{\delta a},\dots,\overline{\delta^{m-1}a})\end{array}$$

induces a bijection $\mathbb{Z}_p/p^m\mathbb{Z}_p\simeq\mathbb{F}_p^m$. For any $\gamma=(\gamma_0,\dots,\gamma_{m-1})\in\mathbb{F}_p^m$ and any $\beta\in I'$, we set

$$v_{\gamma\beta}=\gamma_0^{\beta_0}\gamma_1^{\beta_1}\cdots\gamma_{m-1}^{\beta_{m-1}}\,.$$

Notice that $\delta^i a_\alpha\equiv\delta^i\alpha \bmod p$ if $i\le m-1$. Therefore, by Lemma 11, in order to prove Lemma 12 we just need to show that $\det(v_{\gamma\beta})\neq 0\in\mathbb{F}_p$.

Assume the latter is false. This means that there exist constants $\lambda_{\beta_0\dots\beta_{m-1}}\in\mathbb{F}_p$ for $(\beta_0,\dots,\beta_{m-1})\in I'$, not all zero, such that

$$\sum_{\beta_0=0}^{p-1}\cdots\sum_{\beta_{m-1}=0}^{p-1}\lambda_{\beta_0\dots\beta_{m-1}}\gamma_0^{\beta_0}\gamma_1^{\beta_1}\cdots\gamma_{m-1}^{\beta_{m-1}}=0$$

for all $\gamma\in\mathbb{F}_p^m$. By induction on m, this easily implies that all the λs vanish, a contradiction. This proves our Lemma. □

5. Proof of Theorem 5

We now carry out the proof of Theorem 5 by proving the following result that is more precise. In what follows, I and I' are the sets of indices (5) and (6), respectively.

Theorem 13. *Let $f:\mathbb{Z}_p\to\mathbb{Z}_p$ be an analytic function of level m. Then there exists a unique restricted power series $F\in\mathbb{Z}_p[[x_0,x_1,\dots,x_m]]$ with the following properties:*

1. $F(x_0,x_1,\dots,x_m)=\sum_{n\ge0}\sum_{\beta\in I'}a_{\beta,n}x_0^{\beta_0}x_1^{\beta_1}\cdots x_{m-1}^{\beta_{m-1}}x_m^n$.
2. $f(a)=F(a,\delta a,\dots,\delta^m a)$, $a\in\mathbb{Z}_p$.

Proof. We start by proving the existence of F. Notice that if $g:\mathbb{Z}_p\to\mathbb{Z}_p$ is any arithmetic differential operator of order m and $a\in\mathbb{Z}_p$, then $h(x):=g(x+a)$ is also an arithmetic differential operator of order m; cf. Remark 3, (3). By this, and without losing generality, we may assume that the function f in the statement of the Theorem is zero on all discs of radius $1/p^m$ except for $p^m\mathbb{Z}_p$. Without losing generality also, we may additionally assume that there exists an $l\ge0$ such that $f(p^m u)=u^l$ for all $u\in\mathbb{Z}_p$.

We recall the set C_m in (4). The family of discs $\{a+p^m\mathbb{Z}_p\}_{a\in C_m}$ forms a covering of $\mathbb{Z}_p$. Notice that $a_0 = 0$.

By Lemma 10, for $a \in C_m$ and $0 \leq k \leq m$, we have that $\delta^k(a + p^m u) = \sum_{j=0}^{p^m} c_{a,j}^k u^j$, with $c_{a,0}^k = \delta^k a$, and

$$\left\|c_{a,0}^k\right\|_p \leq 1\,, \quad \left\|c_{a,1}^k\right\|_p = \frac{1}{p^{m-k}}\,, \quad \left\|c_{a,j}^k\right\|_p \leq \frac{1}{p^{(m-k+1)j-1}}\,,\ 2 \leq j \leq p^k\,. \tag{8}$$

We may view $\delta^k(a + p^m u)$ as an element in the ring of polynomials $\mathbb{Z}_p[u]$. Since $\delta^m a = 0$, it follows that $c_{a,j}^m = 0$.

We proceed to inductively determine the coefficients $a_{\beta,n}$ in the series F appearing in the statement of the Theorem, so that

$$\|a_{\beta,n}\|_p \leq \min\left\{1, \frac{1}{p^{n-l}}\right\}\,, \quad n \geq 0\,,\ \beta \in I'\,, \tag{9}$$

and so that, if $F_a(u) = F(a + p^m u)$, for $a \in C_m$, then we have

$$\left\{\begin{array}{rcll} F_a(u) & = & u^l & \text{if} \quad a = 0\,, \\ F_a(u) & = & 0 & \text{if} \quad a \neq 0. \end{array}\right. \tag{10}$$

Here we view (10) as equalities of functions of $u \in \mathbb{Z}_p$. However, since each $F_a(u)$ is defined by a restricted power series in $\mathbb{Z}_p[[u]]$, it is enough to check (10) as equalities in the ring of formal power series $\mathbb{Z}_p[[u]]$.

We consider the polynomials $F_a^k(u) \in \mathbb{Z}_p[u]$ defined by

$$F_a^k(u) := \sum_{n=0}^{k} \sum_{\beta\in I'} a_{\beta,n} \left(\sum_{j=0}^{p^0} c_{a,j}^0 u^j\right)^{\beta_0} \cdots \left(\sum_{j=0}^{p^{m-1}} c_{a,j}^{m-1} u^j\right)^{\beta_{m-1}} \left(\sum_{j=1}^{p^m} c_{a,j}^m u^j\right)^n$$

so that $F_a^k(u)$ converge u-adically to F_a in $\mathbb{Z}_p[[u]]$. We find the $a_{\beta,n}$s inductively so they satisfy the estimate (9), and such that the following congruences hold in the ring $\mathbb{Z}_p[u]$:

$$\left\{\begin{array}{rcllll} F_a^k(u) & \equiv & u^l & \mod & u^{k+1} & \text{if} \quad a = 0\,, \\ F_a^k(u) & \equiv & 0 & \mod & u^{k+1} & \text{if} \quad a \neq 0. \end{array}\right. \tag{11}$$

In what follows we denote by δ_{ij} the Kronecker symbol.

For the starting point of the induction, we choose the coefficients $a_{\beta,0}$, $\beta \in I'$, such that (11) and (9) hold. This can be achieved by solving the system of equations

$$\sum_{\beta\in I'} w_{\alpha\beta} a_{\beta,0} = \delta_{l0}\delta_{\alpha 0}\,, \quad \alpha \in I\,,$$

where $W = (w_{\alpha\beta})$ is the matrix (7). By Lemma 12, this system can be readily solved for the $a_{\beta,0}$s, with the solution being a vector of p-adic integers.

For the k-th step of the induction, let us notice that for $a = a_\alpha$, the coefficient of u^k in $F_a^k(u)$ is given by

$$(c_{a,1}^m)^k \sum_{\beta\in I'} w_{\alpha\beta} a_{\beta,k} + \sum_{n=0}^{k-1} \sum_{\beta\in I'} a_{\beta,n} b_{\beta,n,k}\,, \tag{12}$$

where $b_{\beta,n,k}$ is the coefficient of u^k in

$$\left(\sum_{j=0}^{p^0} c_{a,j}^0 u^j\right)^{\beta_0} \dots \left(\sum_{j=0}^{p^{m-1}} c_{a,j}^{m-1} u^j\right)^{\beta_{m-1}} \left(\sum_{j=1}^{p^m} c_{a,j}^m u^j\right)^n .$$

Thus, $b_{\beta,n,k}$ is a $\mathbb{Z}$-linear combination of products of the form

$$\left(\prod_{i=1}^{\beta_0} c_{a,j_{0i}}^0\right) \dots \left(\prod_{i=1}^{\beta_{m-1}} c_{a,j_{m-1,i}}^{m-1}\right) \left(\prod_{i=1}^{n} c_{a,j_{mi}}^m\right) ,$$

with

$$\sum_{r=0}^{m-1} \sum_{i=1}^{\beta_r} j_{ri} + \sum_{i=1}^{n} j_{mi} = k .$$

We may assume that there are integers s_r such that $j_{ri} \geq 1$ for $i \leq s_r$ and $j_{ri} = 0$ for $i > s_r$. So we have

$$s_r \leq \sum_{i=1}^{s_r} j_{ri} , \quad \sum_{r=0}^{m-1} \sum_{i=1}^{s_r} j_{ri} + \sum_{i=1}^{n} j_{mi} = k . \tag{13}$$

By (8) and the induction hypothesis,

$$\|a_{\beta,n} b_{\beta,n,k}\|_p \leq \min\left\{1, \frac{1}{p^{n-l+\sigma}}\right\} . \tag{14}$$

where

$$\sigma = \sum_{r=0}^{m-1} [(m-r+1)(\sum_{i=1}^{s_r} j_{ri}) - s_r] + \sum_{i=1}^{n} j_{mi} - n .$$

Now, by (13) we have that

$$\begin{aligned} \sigma &\geq \textstyle\sum_{r=0}^{m-1} [2(\sum_{i=1}^{s_r} j_{ri}) - s_r] + \sum_{i=1}^{n} j_{mi} - n \\ &\geq \textstyle\sum_{r=0}^{m-1} \sum_{i=1}^{s_r} j_{ri} + \sum_{i=1}^{n} j_{mi} - n \\ &= k - n . \end{aligned}$$

Hence

$$\|a_{\beta,n} b_{\beta,n,k}\|_p \leq \min\left\{1, \frac{1}{p^{k-l}}\right\} . \tag{15}$$

Now, by the induction hypothesis also, $F_a^k(u)$ satisfies (11) if we have

$$\sum_{\beta \in I'} w_{\alpha\beta} a_{\beta,k} = (c_{a_\alpha,1}^m)^{-k} \left(\delta_{kl}\delta_{\alpha 0} - \sum_{n=0}^{k-1} \sum_{\beta \in I'} a_{\beta,n} b_{\beta,n,k}\right) , \ \alpha \in I. \tag{16}$$

By (8) and (15), the p-adic norm of the right hand side of (16) is bounded above by $\min\{1, 1/p^{k-l}\}$. Again, by Lemma 7, we can solve the system (16) for the $a_{\beta,k}$s, with the solution satisfying the estimates (9). This completes the induction, and hence the existence part of the Theorem.

In order to prove the uniqueness, we need to show that if a restricted power series F satisfies conditions (1) and (2) in the Theorem for $f = 0$, then $a_{\beta,n} = 0$ for all $\beta \in I'$, $n \geq 0$. This follows by an induction on n, in view of the equalities

$$\sum_{\beta \in I'} w_{\alpha\beta} a_{\beta,k} = -(c^m_{a_\alpha,1})^{-k} \left(\sum_{n=0}^{k-1} \sum_{\beta \in I'} a_{\beta,n} b_{\beta,n,k} \right) , \ \alpha \in I.$$

This finishes the proof. □

References

[1] A. Buium, *Arithmetic Differential Equations*, Math. Surveys and Monographs, 118, American Mathematical Society, Providence, RI, 2005. xxxii+310 pp.

[2] A. Buium, *Continuous p-adic functions and p-derivations*, J. Number Theory, 84 (2000), 1, pp. 34-39.

[3] A. Buium, *Differential characters of Abelian varieties over p-adic fields*, Invent. Math. 122 (1995), 2, pp. 309-340.

[4] A. Buium, *Geometry of Fermat adeles*, Trans. Amer. Math. Soc., 357 (2004), pp. 901-964.

[5] A. Buium & S.R. Simanca, *Arithmetic Laplacians*, preprint 2008, arXiv:0805.0256.

[6] A. Buium & S.R. Simanca, *Arithmetic Partial Differential Equations*, preprint 2006, arXiv:math.AP/0605107.

[7] A. Buium & S.R. Simanca, *Arithmetic Partial Differential Equations, II: modular curves*, preprint 2008, arXiv:0804.4856.

[8] P.-J. Cahen & J.-L. Chabert, *Integer Valued Polynomials*, Mathematical Surveys and Monographs, 48. American Mathematical Society, Providence, RI, 1997. xx+322 pp.

[9] K. Conrad, *The digit principle*, J. Number Theory, 84 (2000), 2, pp. 230-257.

[10] K. Mahler, *Introduction to p-adic numbers and their functions*, CTM 64, Cambridge University Press, 1973.

[11] J-P. Serre, *Lie algebras and Lie groups*, Benjamin, New York, 1965.

Department of Mathematics & Statistics, The University of New Mexico, NM 87131

E-mail addresses: buium@math.unm.edu, cralph@unm.edu, santiago@math.unm.edu